Notice of Allowability	Application No.	Applicant(s)	
	09/930,903	CAMPAGNA, MATTHEW	
	Examiner	Art Unit	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *interview on April 14, 2005*.

2. ☒ The allowed claim(s) is/are *6-8, 10-12 and 37*.

3. ☒ The drawings filed on *8/17/2001* are accepted by the Examiner.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 210[illegible]

DETAILED ACTION

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

2. Authorization for this examiner's amendment was given in a telephone interview with Charles R. Malandra, Jr. on 4/14/2005.

The application has been amended as follows:

3. Please cancel claims 1 – 5.

4. Please replace claim 6 with the following:

Claim 6. A method for sending a message, said method comprising the steps of:

a) generating by a sender a password P;

b) sending the password P to a message recipient over a first channel;

c) generating authentication information by the sender for server authentication of the message recipient, wherein the authentication information is dependent on knowing the password P;

d) generating by the sender a random number as an initialization vector IV4;

e) generating by the sender a private key PK as H(IV4 | P), where P is a password known to a message recipient, H( ) is an agreed upon hashing algorithm and (|) is a message concatenation;

f) generating by the sender an encryption ENC = E(M | H(M), PK), where E is a predetermined symmetric key encryption algorithm, M is the message;

g) sending the authentication information and (IV4, ENC) from the sender to the server over a second channel;

h) authenticating the message recipient over a third channel using the authentication information to verify that the message recipient knows the password P; wherein the authentication information comprises:

h-1) the authentication response AR as E(ACNST2, ARK) generated by the message recipient, where ACNST2 is a predetermined constant;

h-2) the authentication response key ARK as H(IV2 | IV3 | AS), where IV2 is a second random number (as a second initialization vector) generated by the server and IV3 is a third random number (as a third initialization vector) generated by the message recipient;

h-3) the authentication string AS is E(ACNST1, PK), where ACNST1 is a predetermined constant and E is a predetermined symmetric key encryption algorithm.

i) sending ENC from the server to the message recipient over the third channel only when the message recipient has been authenticated by the server.

5. Please replace claim 8 with the following:

Claim 8. A method as described in claim 6 wherein step c) further comprises the steps of:

i) generating by the sender a first random number as a first initialization vector IV1;

ii) generating by the sender H(IV1 | P) as an authentication key AK;

iii) generating by the sender an authentication string AS as E(ACNST1, AK), where ACNST1 is a predetermined constant and E is a predetermined symmetric key encryption algorithm;

and wherein step g) further comprises the steps of sending IV1 and AS to the server over the second channel:

and wherein step h) further comprises the steps of:

iv) sending from the server said vectors IV1 and IV2 to said message recipient over the third channel;

v) regenerating by said message recipient the authentication key AK;

vi) regenerating by said message recipient the authentication string AS;

vii) sending from said message recipient to the server IV3 and AR;

viii) regenerating by the server the authentication response key ARK as H(IV2 | IV3 | AS);

ix) computing by the server a decryption D(AR, ARK), where D is a symmetric decryption algorithm corresponding to E; and

x) authenticating said message recipient only if D(AR, ARK) = ACNST2, where ACNST2 is a second predetermined constant;

and wherein step i) comprises the steps of:

xi) generating D(ENC, PK) = (M | H(M)), where D is a symmetric key decryption algorithm corresponding to E;

xii) calculating H(M) from said value of M generated in step c; and

xiii) accepting said generated value of M only if said calculated value of H(M) equals said value of H(M) generated in step c).

6. Please cancel claim 9.

7. Please cancel claims 13 – 36.

8. Please add a new claim 37 as the following:

Claim 37. A system for sending a message, said system comprising:

a) means for generating by a sender a password P;

b) means for sending the password P to a message recipient over a first channel;

c) means for generating authentication information by the sender for server authentication of the message recipient, wherein the authentication information is dependent on knowing the password P;

d) means for generating by the sender a random number as an initialization vector IV4;

e) means for generating by the sender a private key PK as H(IV4 | P), where P is a password known to a message recipient, H( ) is an agreed upon hashing algorithm and (A|B) is a message concatenation;

f) means for generating by the sender an encryption ENC = E(M | H(M), PK), where E is a predetermined symmetric key encryption algorithm, M is the message;

g) means for sending the authentication information and (IV4, ENC) from the sender to the server over a second channel;

h) means for authenticating the message recipient over a third channel using the authentication information to verify that the message recipient knows the password P; wherein the authentication information comprises:

h-1) the authentication response AR as E(ACNST2, ARK) generated by the message recipient, where ACNST2 is a predetermined constant;

h-2) the authentication response key ARK as H(IV2 | IV3 | AS), where IV2 is a second random number (as a second initialization vector) generated by the server and IV3 is a third random number (as a third initialization vector) generated by the message recipient;

h-3) the authentication string AS is E(ACNST1, PK), where ACNST1 is a predetermined constant and E is a predetermined symmetric key encryption algorithm.

i) means for sending ENC from the server to the message recipient over the third channel only when the message recipient has been authenticated by the server.

Allowable Subject Matter

9. Claims 6 – 8, 10 – 12 and 37 are allowed.

10. The following is an examiner's statement of reasons for allowance:

The above mentioned claims are allowable over prior arts because the CPA (Cited Prior Art) of record fails to teach or render obvious the claimed limitations in combination with the specific added limitations, as recited in independent claim 6 and subsequent dependent claims.

The CPA does not teach or suggest a system for providing, by a sender, a password P and sending the password P to a message recipient over a first channel; generating authentication information by the sender for server authentication of the message recipient, wherein the authentication information is dependent on knowing the password P; generating by the sender a random number as an initialization vector IV4; generating by the sender a private key PK as H(IV4 | P), where P is a password known to a message recipient, H( ) is an agreed upon hashing algorithm and (A|B) is a message concatenation; generating by the sender an encryption ENC = E(M | H(M), PK), where E is a predetermined symmetric key encryption algorithm, M is the message; sending the authentication information and (IV4, ENC) from the sender to the

server over a second channel; authenticating the message recipient over a third channel using the authentication information to verify that the message recipient knows the password P; wherein the authentication information comprises:

a) the authentication response AR as E(ACNST2, ARK) generated by the message recipient, where ACNST2 is a predetermined constant;

b) the authentication response key ARK as H(IV2 | IV3 | AS), where IV2 is a second random number (as a second initialization vector) generated by the server and IV3 is a third random number (as a third initialization vector) generated by the message recipient;

c) the authentication string AS is E(ACNST1, PK), where ACNST1 is a predetermined constant and E is a predetermined symmetric key encryption algorithm; and

sending ENC from the server to the message recipient over the third channel only when the message recipient has been authenticated by the server.

Claim 37 would also be allowable for the reasons stated above.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131

LBC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100